



J. TYLER McCAULEY
AUDITOR-CONTROLLER

COUNTY OF LOS ANGELES DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-2766
PHONE: (213) 974-8301 FAX: (213) 626-5427

June 6, 2002

TO: Supervisor Zev Yaroslavsky, Chairman
Supervisor Gloria Molina
Supervisor Yvonne Brathwaite Burke
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: J. Tyler McCauley *by RJM*
Auditor-Controller

SUBJECT: **Review of Internal Services Department's Disaster Recovery Plan**

We have completed a review of the Internal Services Department's (ISD) Disaster Recovery Plan for its mainframe and network computer operations.

ISD's Information Technology Services (ITS) Branch operates one of the largest data centers in the western United States. Over 3.9 million transactions are processed each day through more than 25,000 terminals linked by an extensive communications network. ITS utilizes a wide variety of hardware and software, including IBM and Unisys mainframes, midrange computers, and various personal computers and workstations to support the County's computing needs. In addition, ITS implements new technologies such as Internet access, electronic mail (email), distributed computing, and optical storage.

Scope

Our review focused on evaluating whether the Department's Disaster Recovery Plan is comprehensive enough to ensure that business interruptions are minimized in the event of a disaster by restoring critical systems and files, computer output services and telecommunications. Disasters that could disable computing operations include events such as earthquakes, power outages, vandalism, fires, sabotage, and hackers. In addition, we reviewed the Disaster Recovery Plan to ensure it contained those components of an effective Business Continuity Plan that relate to data processing and telecommunications.

Based on the results of our review of ISD's Plan, we expanded our review to evaluate the extent to which a Countywide Disaster Recovery Plan exists. We also followed up

on recommendations contained in ISD's 1999 COMDISCO Report. ISD contracted with COMDISCO, an outside consultant, to conduct an assessment of ISD's data center's suitability as the County's primary data center. In addition, we examined whether intrusion and detection systems were in place and functioning as intended.

Summary of Findings/Recommendations

Countywide Disaster Recovery Standards

According to the Chief Administrative Officer's (CAO) Office of Emergency Management, departments are responsible for developing their own disaster recovery policies. Countywide system recovery priorities do not exist to assist departments in coordinating their disaster recovery plans. As a result, departments will need to find alternative methods of handling their tasks, which may result in a disruption of delivering critical services. Citing the difficulties of ranking their customers' systems, ISD has not taken the lead to develop Countywide system recovery priorities. In addition, ISD does not maintain all County systems. Departments such as Public Social Services (DPSS), Health Services (DHS), and Sheriff are responsible for maintaining most of their own systems.

The Chief Information Officer (CIO) is responsible for recommending adoption of standards for Countywide information technology subject to the approval of the Board of Supervisors. Accordingly, we have recommended that the Board of Supervisors direct the CIO to establish a task force comprised of the CAO, ISD and other affected County departments to develop Countywide Disaster Recovery Plan Standards that incorporate those components of a Business Continuity Plan that relate to data processing and telecommunications. Once these Standards have been developed and approved by the Board of Supervisors, the CIO, CAO and ISD should ensure each County department develops and maintains an internal plan for compliance with those Standards.

Countywide Business Impact Analysis

The Disaster Recovery Plan should not only emphasize the resumption of information systems, but also focus on the uninterrupted maintenance of critical business processes (business continuity). The first step in enabling management to move from a position of data processing recovery to business continuity is a business impact analysis (BIA).

The BIA should identify those systems that, if rendered inoperable, would inhibit the County's ability to deliver mission critical services and ensure those systems are prioritized logically. Therefore, system recovery priorities should coincide with the types of services that the County considers the most important, such as public safety and health care.

A Countywide BIA does not exist to guide the County. The BIA is needed to identify the key business processes, the priorities assigned to the processes, and the quantified impact of business disruptions so that resources can be devoted to recovering the most important systems.

A BIA will have a higher probability of success if the Board of Supervisors instructs the CIO, CAO, ISD and other affected County departments to be involved in its development. Accordingly, we have recommended that the Board of Supervisors instruct the Disaster Recovery Standards Task Force recommended above to develop a Countywide BIA that addresses disaster recovery issues and specific recovery priorities for all departments.

ISD's Disaster Recovery Plan

Our review disclosed that ISD's Disaster Recovery Plan is not comprehensive and either does not address, or does not adequately address, several key areas. The following are areas where ISD needs to make improvements in the Plan to ensure the County can adequately recover from a disaster:

- **Business Impact Analysis (BIA)** - ISD and user departments have not identified critical systems, processes and functions; assessed the economic impact of incidents and disasters; or estimated the length of time business units can survive without access to their systems, services and facilities.
- **Critical Systems** - ISD and user departments have not identified and ranked critical systems from highest to lowest priority, including required recovery times.
- **Alternate Data Storage Sites** - 20% of ISD's IBM application programs and data are not maintained at an off-site location.
- **Telecommunication Requirements** - ISD's Disaster Recovery Plan does not include a discussion of telecommunication network recovery requirements, including telephone voice circuits, wide area networks, and local area networks.
- **Communication Bandwidth Requirements** - ISD has not estimated the total bandwidth required to communicate with the hot-site(s) during disaster recovery operations.
- **Critical Systems Tests** - Although critical Unisys systems have been fully tested and recovered at the remote hot-site, many critical IBM systems have not.
- **Disaster Recovery Plan Updates** - Although system recovery procedures are updated regularly, ISD's Disaster Recovery Plan is not reviewed and updated on a periodic basis to reflect changing requirements.
- **Emergency Output Services Supplies** - ISD and user departments do not have sufficient emergency blank warrant stock on-hand for continuing business activity during a disaster that lasts for an extended period. In

addition, ISD has not developed and included contingency plans for its computer output operations in the Disaster Recovery Plan. Any prolonged interruptions or failure to provide computer output services to user Departments could severely impact the County's operations.

We also noted that ISD has relied on disaster recovery coordinators with technical knowledge to coordinate the mainframe and telecommunications disaster recovery. However, no other staff have been trained to replace these individuals in the event they are unavailable.

ISD recognizes that the current Disaster Recovery Plan is not sufficient to ensure County operations can recover efficiently and effectively in the event of a disaster. As an alternative, ISD relies on test scripts, schedules, diagrams, memos and reports maintained by several individuals. Although these documents are usable to some extent, this collection of critical documents would be difficult to use during a disaster. In addition, they are difficult to update and use for training purposes.

We have recommended that a new Disaster Recovery Plan be developed that incorporates existing documents as well as documentation that explains what ISD's recovery priorities are and the methodology and staffing to be used. The Plan should conform to the Countywide Disaster Recovery Standards once they are developed as recommended in this report. ISD's Plan should include ISD's mainframe and midrange systems, network infrastructure system, telecommunications and output services. In addition, ISD should ensure the Disaster Recovery Plan designates trained backup personnel for the disaster recovery coordinators. The Disaster Recovery Plan should also be reviewed and updated quarterly, or as major changes occur, to ensure that it is current and complete.

Additional Issues

We have also recommended that ISD investigate the feasibility of using data mirroring to backup IBM systems and programs. Data mirroring is a technique that allows data to be copied from one location to a remote storage device in real time. In the event of a disaster, use of data mirroring can significantly reduce recovery time of critical data from days to hours.

In addition, we noted that the CAO, ISD and the Department of Public Works (DPW) are currently in the process of planning a new data center and estimate it will take three to five years to complete. In the interim, ISD has taken measures to upgrade their current data center by implementing the recommendations from the COMDISCO Report that are cost beneficial.

These and other findings and recommendations are discussed in detail in the attached report.

Review of Report

We discussed the results of our review with ISD and CIO management. Their written responses (attached) indicate general agreement with our recommendations and intent to pursue their implementation. The CIO has indicated that the duties of the Disaster Recovery Standards Task Force should include Business Continuity Planning Standards for all operations not just data processing and telecommunications. We agree and have already begun an assessment of the Auditor-Controller's ability to continue all operations in the event of a disaster.

We thank ISD and CIO management and staff for their cooperation and assistance during our review.

If you have any questions, please contact me or your staff may contact DeWitt Roberts at (213) 974-0301, or Ian Clark at (213) 974-0303.

JTM: PTM: DR
Attachment

c: David E. Janssen, Chief Administrative Officer
Joan Ouderkirk, Director, Internal Services Department
Jon W. Fullinwider, Chief Information Officer
Violet Varona-Lukens, Executive Officer
Public Information Office
Audit Committee

Internal Services Department Disaster Recovery Plan Review

Comments and Recommendations

Background

The Internal Services Department's (ISD) Information Technology Services (ITS) Branch operates one of the largest data centers in the western United States. Over 3.9 million transactions are processed each day through more than 25,000 terminals linked by an extensive communications network. ITS utilizes a wide variety of hardware and software, including IBM and Unisys mainframes, midrange computers, and various personal computers and workstations to support the County's computing needs. In addition, ITS implements new technologies such as Internet access, electronic mail (email), distributed computing, and optical storage.

ITS provides County departments with essential information technology and communication services that are critical to the County's mission of serving the public. ITS supports diverse systems such as the Countywide Timekeeping and Payroll/Personnel System (CWTAPPS), the Adult Probation System, and other systems providing critical information for the Department of Health Services (DHS), the District Attorney's Office, the Assessor, etc. ISD also provides user departments' access to the Internet, email, and midrange systems.

Certain systems, such as the California Law Enforcement Telecommunications System, and Automated Justice Information System, as well as others, are considered critical to County operations. If a disaster disables ISD's data center, the operation of these systems would have to be recovered within a relatively short period of time to ensure restoration of essential County services.

Scope

We performed a review of ISD's Disaster Recovery Plan for its mainframe and network computer operations. Our review focused on evaluating whether the Disaster Recovery Plan is comprehensive enough to ensure that business interruptions can be minimized in the event of a disaster by restoring critical systems and files, computer output services and telecommunications. Disasters that could disable computing operations include events such as earthquakes, power outages, vandalism, fires, sabotage and hackers. In addition, we reviewed the Disaster Recovery Plan to ensure it contained those components of an effective Business Continuity Plan that relate to data processing and telecommunications. The essential components of a Disaster Recovery Plan include:

- Identifying key decision-making personnel and maintaining their telephone numbers and addresses.
- Maintaining required materials for continuing normal business activities.

- Organizing Teams for Emergency Action, Damage Assessment, Emergency Management, Security, Emergency Operations, Network Recovery, and User Hardware.
- Preparing a Business Impact Analysis (BIA) that will identify critical business functions and ranking those systems in order of importance.
- Identifying critical recovery time in which business processing must be resumed.
- Acquiring and maintaining an off-site storage facility for backup media required for the recovery process.
- Selecting alternate computer hardware and software sites, including a hot-site that is fully configured and ready to operate in a few hours.
- Ensuring adequate telecommunications exists, including telephone voice circuits, wide area networks and local area networks.
- Annual testing and maintenance of the Disaster Recovery Plan, which includes determining how well the Disaster Recovery Plan works or which portions of the Disaster Recovery Plan need improvement.

A listing summarizing ISD's compliance with the components of an effective Disaster Recovery Plan is included in Attachment A and is more fully discussed in the body of this report.

We also followed up on recommendations contained in ISD's 1999 COMDISCO Report. ISD contracted with COMDISCO, an outside consultant, to conduct an assessment of ISD's data center's suitability as the County's primary data center. In addition, we examined whether intrusion and detection systems were in place and functioning as intended.

Our detailed findings and recommendations are discussed below.

Development of Countywide Disaster Recovery Standards

In 1999, the Board of Supervisors (Board) instructed ISD, the Chief Administrative Office (CAO) and the Chief Information Office (CIO) to acquire the services of a consultant to review and update ISD's Disaster Recovery Plan for both the IBM and Unisys systems and develop a proposal for a Countywide Disaster Recovery Plan. The purpose of creating a Countywide Disaster Recovery Plan was to develop a comprehensive Disaster Recovery Plan that encompassed localized and regional disaster, critical end-user access, critical system processing, and recovery priorities.

Our review disclosed that the Disaster Recovery Plan is not comprehensive and either does not address or does not adequately address several key areas as discussed in detail later in this report. According to the CAO's Office of Emergency Management,

departments are responsible for developing their own disaster recovery policies. Countywide system recovery priorities do not exist to assist departments in coordinating their disaster recovery plans. As a result, departments will need to find alternative methods of handling their tasks, which may result in a disruption of delivering critical services. Citing the difficulties of ranking their customers' systems, ISD has not taken the lead to develop Countywide system recovery priorities. In addition, ISD does not maintain all County systems. Departments such as Public Social Services (DPSS), DHS, and the Sheriff are responsible for maintaining most of their own systems.

The CIO is responsible for recommending adoption of standards for Countywide information technology subject to the approval of the Board of Supervisors. Accordingly, the Board of Supervisors should direct the CIO to establish a task force comprised of the CAO, ISD and other affected departments to develop Countywide Disaster Recovery Plan Standards that incorporates those components of an effective Business Continuity Plan that relate to data processing and telecommunications. Once these Standards have been developed and approved by the Board of Supervisors, the CIO, CAO and ISD should ensure each County department develops and maintains an internal plan for compliance with those Standards.

Recommendations

1. **Board of Supervisors direct the CIO to establish a task force comprised of the CAO, ISD, and other affected departments to develop Countywide Disaster Recovery Plan Standards that incorporate those components of an effective Business Continuity Plan that relate to data processing and telecommunications.**
2. **The CIO, CAO and ISD ensure each County department develops and maintains an internal plan for compliance with those Standards once these Countywide Disaster Recover Plan Standards are developed and approved.**

Business Impact Analysis

The Disaster Recovery Plan should not only emphasize the resumption of information systems, but also focus on the uninterrupted maintenance of critical business processes (business continuity). The first step in enabling management to move from a position of data processing recovery to business continuity is a business impact analysis (BIA).

The BIA should identify those systems that, if rendered inoperable, would inhibit the County's ability to deliver mission critical services and ensure those systems are prioritized logically. Therefore, system recovery priorities should coincide with the types of services that the County considers the most important, such as public safety and health care.

A Countywide BIA does not exist to guide the County. The BIA is needed to identify the key business processes, the priorities assigned to the processes, and the quantified

impact of business disruptions so that resources can be devoted to recovering the most important systems.

A BIA will have a higher probability of success if the Board of Supervisors instructs the CIO, the CAO, and ISD and other affected County departments to be involved in its development. The Board of Supervisors should instruct the Disaster Recovery Standards Task Force recommended above to develop a Countywide BIA that addresses disaster recovery issues and specific recovery priorities for all departments.

Recommendation

- 3. Board of Supervisors instruct the Disaster Recovery Standards Task Force recommended above to develop a Countywide BIA that addresses disaster recovery issues and specific recovery priorities for all departments.**

ISD's Disaster Recovery Plan

As previously stated, we reviewed ISD's Disaster Recovery Plan for its mainframe and network computer operations. Our review focused on evaluating whether the Disaster Recovery Plan is comprehensive enough to ensure that business interruptions can be minimized in the event of a disaster by restoring critical systems and files, computer output services and telecommunications. Our review disclosed that the Disaster Recovery Plan is not comprehensive and either does not address or does not adequately address several key areas. The following are areas where improvements are needed to ensure the County can adequately recover from a disaster:

- **Business Impact Analysis** - ISD and user departments have not identified critical systems, processes and functions; assessed the economic impact of incidents and disasters; or estimated the length of time business units can survive without access to their systems, services and facilities.
- **Critical Systems** - ISD and user departments have not identified and ranked critical systems from highest to lowest priority, including required recovery times.
- **Alternate Data Storage Sites** - 20% of ISD's IBM application programs and data are not maintained at an off-site location.
- **Telecommunication Requirements** - ISD's Disaster Recovery Plan does not contain a discussion of telecommunication network recovery requirements, including telephone voice circuits, wide area networks, and local area networks.
- **Communication Bandwidth Requirements** - ISD has not estimated the total bandwidth required to communicate with the hot-site(s) during disaster recovery operations.

- **Critical Systems Testing** - Although critical Unisys systems have been fully tested and recovered at the remote hot-site, many critical IBM systems have not.
- **Disaster Recovery Plan Updates** - Although system recovery procedures are updated regularly, ISD's Disaster Recovery Plan is not reviewed and updated on a periodic basis to reflect changing requirements.
- **Emergency Output Services and Supplies** - ISD and user departments do not have sufficient emergency blank warrant stock on-hand for continuing business activity during a disaster that lasts for an extended period of time. In addition, ISD has not developed and included contingency plans for its computer output operations in their Disaster Recovery Plan. Any prolonged interruptions or failure to provide computer output services to user Departments could severely impact the County's overall business.

We also noted that the Disaster Recovery Plan states that the Disaster Recovery Plan should be reviewed and updated at least quarterly, or as major changes occur. However, the appendices to the Plan include Emergency Action Team lists that have not been updated to reflect changes in the staff assignments and contact numbers. For example, we noted one individual who was designated as a team leader had not received any training and was unaware of his assignment.

We also noted ISD has relied on disaster recovery coordinators with technical knowledge to coordinate the mainframe and telecommunications disaster recovery. However, there are no other staff trained to replace these individuals in the event they are unavailable.

ISD recognizes that the current Disaster Recovery Plan is not sufficient to ensure County operations can recover in the event of a disaster. As an alternative to the Disaster Recovery Plan, ISD relies on test scripts, schedules, diagrams, memos and reports maintained by several individuals. Although these documents are usable to some extent, this collection of critical documents would be difficult to use during a disaster. Also, they are difficult to update and use for training purposes. Therefore, a new Disaster Recovery Plan should be developed that incorporates these existing documents as well as documentation that explains what ISD's recovery priorities are and the methodology and staffing to be used. The plan should include ISD's mainframe and midrange systems, network infrastructure system, telecommunications and output services.

In addition, ISD should ensure the Disaster Recovery Plan includes designated backup personnel for the disaster recovery coordinators. The Disaster Recovery Plan should be reviewed and updated quarterly, or as major changes occur, to ensure that it is current and complete. Also, ISD management should provide training for Emergency Action Teams to reinforce staff assignments and the actions to be taken by Team members.

Recommendations

- 4. ISD management develop a formal comprehensive Disaster Recovery Plan that addresses the problem areas discussed in this report.**
- 5. ISD management review and update the Disaster Recovery Plan quarterly, or as major changes occur.**
- 6. ISD management ensure the Disaster Recovery Plan includes designated backup personnel for the disaster recovery coordinators.**
- 7. ISD management provide training for Emergency Action Teams to reinforce staff assignments and the actions to be taken by Team members.**

Hot-site Testing

ISD has agreements with two vendors, COMDISCO and Sungard, to provide disaster recovery services for its IBM and Unisys based systems with separate hot-sites located in two areas outside of the State. A "hot-site" is a primary, fully operational, data processing facility, containing an installed computer equipment configuration that meets the user's specifications. Hot-site agreements stipulate that fully operational data processing facilities will be immediately available for use in the event of a disaster. The agreements also provide a certain number of hours allowed for testing the capabilities of the hot-sites.

At the time of ISD's evaluation for disaster recovery services, the following three vendors were considered: IBM, COMDISCO, and Sungard. Of the three, Sungard was the only vendor that could support both the IBM and Unisys platforms. However, ISD management indicated that Sungard's proposal to provide for IBM platform recovery was too costly. Therefore, ISD contracted with COMDISCO for the IBM platform recovery and Sungard for the Unisys platform recovery. These two vendors have subsequently merged into one company, Sungard. However, the hot-sites have not been merged.

At the time of the evaluation, ISD considered contracting disaster recovery services from a single vendor. Contracting with a single vendor for disaster recovery services offers several advantages. For example, the hot-site testing could be performed at one location rather than two, which would result in the simplification of disaster recovery efforts. Other advantages include establishing communication links and simplification of overall disaster recovery coordination. Now that ISD managers have had an opportunity to work with two separate locations, the advantages of a single location have become more apparent. Due to the advantages of a single location, ISD management should pursue with Sungard consolidating their two hot-site locations to one locality.

Recommendation

- 8. ISD management pursue with Sungard consolidating their two hot-site locations to one locality.**

Disaster Recovery Plan Testing

Disaster Recovery Plan testing provides important benefits. It assists in determining if the Disaster Recovery Plan is accurate and provides reassurance that operations will continue in the event of a disaster. It also discloses weaknesses in the Disaster Recovery Plan such as the lack of availability of data and programs necessary for recovery, limitations of the computing capabilities and capacity at the hot-sites, inadequate recovery planning, and lack of awareness of the individual responsibilities of recovery staff. A good Disaster Recovery Plan requires at least annual testing.

ISD has regularly tested the capabilities of the Unisys hot-site for the last six years and believes that the majority of the Unisys systems would be recovered in the event that a disaster occurs. In March 2001, we observed ISD's and the Child Support Services Department's (CSSD) test of its primary computer system, the Automated Child Support Enforcement Replacement System (ARS), which accounts for 90% of the Unisys workload. The test successfully allowed CSSD to reroute their processing and communications to the hot-site.

We did note that ISD and CSSD conducted disaster recovery tests from each Department's regular workstations using documentation normally available to them. To provide a better simulation of an actual disaster and the eventual restart and recovery of the critical systems, ISD should conduct unannounced offsite testing using documentation, files and programs that are only available at the offsite locations.

Recommendation

- 9. ISD management conduct unannounced offsite testing using documentation, files and programs that are only available at the offsite locations.**

Because the Unisys environment is comprised of only a few systems, it is easier to perform regular disaster recovery tests. The IBM environment is comprised of over 200 systems, making it much more difficult for ISD to perform tests on all systems in this environment. ISD has only tested three (less than 2%) IBM based systems in the last four years, for functional hot-site recovery. The selection of these systems was not based on a formally defined testing schedule. For example, the Department of Mental Health's Management Information System (MHMIS) was tested as a result of an Auditor-Controller (A-C) audit report recommendation. The other two systems, the A-C's Countywide Payroll System and the Countywide Timekeeping and Payroll/Personnel System were tested as part of the pilot to determine if ISD could recover a Countywide system.

Unless a test schedule is developed, the same three Unisys systems may continue to be tested each year. Since it would not be practical to test the recovery capabilities of every system because testing at the hot-sites is contractually limited, ISD management should work with the user departments to develop a formal hot-site testing schedule for high priority Unisys and IBM systems using the BIA (See Recommendation 3).

Recommendation

- 10. ISD management work with the user departments to develop a formal hot-site testing schedule for high priority Unisys and IBM systems using the BIA (See Recommendation 3).**

Data Mirroring

According to ISD, because the County's IBM environment is comprised of many smaller systems from several departments, it could not ensure that all system information is being captured and sent off-site to storage or that all critical data could be recovered timely in the event of a disaster. The current data restoration process takes several days to complete.

ISD does not currently use data mirroring, a technique that allows data to be copied from one location to a remote storage device in real time. In the event of a disaster, use of data mirroring can significantly reduce recovery time of critical data. According to ISD, data mirroring would allow a complete backup of all IBM applications and reduce the recovery time from days to hours. ISD management should determine the feasibility of using data mirroring on IBM applications to significantly reduce data recovery time.

Recommendation

- 11. ISD management determine the feasibility of using data mirroring on IBM applications to significantly reduce data recovery time.**

Computer Output Services

ISD provides computer output services for 43 County departments. Computer output services include laser printing, microfiche, impact printing, and xerography. ISD is responsible for the production and delivery of outputs such as payroll and welfare warrants, tax bills, property assessments and various reports vital to the day-to-day operations of several County departments. Any prolonged interruptions or failure to provide computer output services to these departments could severely impact the County's overall business. The County's reliance on continuous output services requires that ISD have contingency plans in place to restore these services in the event of a disaster.

Our review disclosed that ISD has not developed and included contingency plans for its computer output operations in the Department's Disaster Recovery Plan. ISD management indicated that because the data center's output configuration is highly customized and uses various data streams, implementing a backup output capability

has been extremely difficult. Previously, ISD contracted their disaster recovery for output services to three vendors that resulted in only 40% coverage of its total workload. Currently, ISD does not have a contract with any vendor that would provide output services in the event a disaster.

Although ISD is in the process of reducing the risk of losing output capability by using high-speed laser printers in place of slower impact printers, streamlining data traffic, and using more network printers, completion of these projects is not expected for another five years. The risk of not completing these projects earlier adversely affects the County's ability to restore services if a disaster were to occur. Therefore, ISD management should place a higher priority in replacing impact printers with laser printers, streamlining data traffic and using more network printers.

ISD management needs to ensure that computer output recovery operations are developed and coincide with the system recovery priorities and include them in the Disaster Recovery Plan. It should be noted that not all systems would be recovered in an event of a disaster. As a result, County departments will need to find alternative methods of handling their tasks, which may result in a disruption of delivering critical services. Therefore, ISD management should work closely with user departments to develop contingency plans including evaluation/feasibility of user departments using alternative methods to handle tasks if critical automated output services are inoperable for a significant period of time.

Recommendations

- 12. ISD management place a higher priority in replacing impact printers with laser printers, streamlining data traffic and using more network printers.**
- 13. ISD management ensure that computer output recovery operations are developed and coincide with the system recovery priorities and include them in the Disaster Recovery Plan.**
- 14. ISD management work closely with user departments to develop contingency plans including evaluation/feasibility of user departments using alternative methods to handle tasks if critical automated output services are inoperable for a significant period of time.**

Telecommunications Recovery

ISD's Telecommunications Branch is responsible for ensuring that County departments can maintain communication with each other, other governmental agencies, and the public. Its primary responsibility is for the continued operation and maintenance of the LAinternet (LANet). LANet is the County's wide area network and is connected by routers used for the transmission of data, voice and images. A router is an intelligent device that manages the flow of data between networks.

Our review disclosed that ISD only has two router locations within the County and does not have additional (backup) routers that can connect to the COMDISCO and Sungard hot-sites. The absence of additional router locations increases the vulnerability that a single event would disrupt telecommunication services for all or a major portion of ISD's customers. ISD acknowledged that, if these two locations were rendered inoperable, the County's networks would be disabled and the connection to the hot-sites would be lost.

If ISD's data processing center is disabled, ISD intends to connect to the hot-sites through a primary LANet router located outside the data center. Consequently, all of ISD's hot-site testing has been conducted with the assumption that this location will remain operable. However, damage can range from localized/minor to widespread, including disabling of the primary router location. Because of the importance of this site, alternative locations should be identified and tested to eliminate potential single points of failure.

To better prepare for a disaster, ISD management should ensure the Disaster Recovery Plan includes additional router locations other than the primary LANet router sites and determine how to connect them to the hot-site(s). Also, ISD management should conduct hot-site testing of the additional router locations to verify that they are viable and include them with the regularly scheduled testing.

Recommendations

- 15. ISD management ensure the Disaster Recovery Plan includes additional router locations other than the primary LANet router sites and determine how to connect them to the hot-site(s).**
- 16. ISD management conduct hot-site testing of the additional router locations to verify that they are viable and include them with the regularly scheduled testing.**

In the event of a disaster, ISD intends to use dedicated telecommunication lines to handle the current data center workload capacity. However, the number of lines planned may not be sufficient to handle current workload. ISD indicated that there have been discussions regarding bandwidth (workload capacity), including requesting additional telecommunication lines or expanding bandwidth, but they have not developed a formal Disaster Recovery Plan to determine what is required to handle the current workload. ISD management should conduct an analysis to determine the bandwidth required of the telecommunication lines needed for disaster recovery purposes and include it in the Disaster Recovery Plan.

In addition, ISD's disaster recovery service contracts with COMDISCO and Sungard do not contain provisions for additional lines to be made available. Also, there are no provisions in the contracts stating how quickly additional lines should be made available or any indication that the vendor would be able to make them available. Staff involved with testing indicated that acquiring additional lines would take weeks or even months in

normal situations and would likely take longer following a disaster. It is uncertain whether user departments are aware of these bandwidth issues.

Modifying the existing agreements with the vendors to increase the number of telecommunication lines in the event of a disaster would allow ISD to quickly increase bandwidth. ISD management should modify the disaster recovery services contracts with COMDISCO and Sungard to include emergency or contingency provisions for adding additional telecommunication lines.

Recommendations

- 17. ISD management conduct an analysis to determine the bandwidth required of the telecommunication lines needed for disaster recovery purposes and include it in the Disaster Recovery Plan.**
- 18. ISD management modify the disaster recovery services contracts with COMDISCO and Sungard to include emergency or contingency provisions for adding additional telecommunication lines.**

Network Infrastructure System

The Network Infrastructure System (NIS) is a system that supports networked computers, routers, switches and firewalls located at ISD's data center. The NIS is used as the gateway to establish a connection for users to interface with ISD's data center computing resources. County departments and vendor personnel are connected through the NIS to access Internet and email services as well as applications running on the IBM and Unisys mainframes and midrange computers.

Our discussions with ISD's Technology Division disclosed that for other than mainframe connectivity for County departments, the NIS is not included in ISD's Disaster Recovery Plan. Also, their agreements with Sungard and IBM do not provide a backup for the NIS. An interruption in the NIS would disable all communication capabilities to the mainframe computers for external vendors such as Affiliated Computer Systems (ACS), which provides updates to other systems for welfare payment services. It would also eliminate access to midrange computers for County departments such as the Sheriff, as well as email and Internet services for County users.

ISD management should determine if the individual components of the NIS could be recovered independently. This would allow connectivity to services available through the NIS to be reestablished on a priority basis. Since the NIS is necessary for users to access vital applications, ISD management should ensure that all components of the NIS are included in the Disaster Recovery Plan. Also, ISD management should determine the methodology required to recover the NIS components on a priority basis in the Disaster Recovery Plan.

Recommendations

19. **ISD management determine if the individual components of the NIS could be recovered independently.**
20. **ISD management ensure that all components of the NIS are included in the Disaster Recovery Plan.**
21. **ISD management determine the methodology required to recover the NIS components on a priority basis in the Disaster Recovery Plan.**

Midrange Computers

ISD's midrange computing resources consist of over 150 Windows NT, Internet and email servers that run the Department's mission critical systems (e.g., Marshall Automated Information System) from the data center. Our review disclosed that midrange computers are not included in ISD's Disaster Recovery Plan. In addition, ISD does not have written agreements with any vendors to provide disaster recovery services, including hot-site agreements, for its midrange computers. In addition, there are no other contingencies for restoring the midrange computing resources if a disaster occurs. ISD management indicated that although data is stored offsite, they do not have a formal Disaster Recovery Plan or agreement to obtain the hardware necessary to recover data in the event of a disaster.

ISD management should investigate the feasibility of obtaining an agreement with a vendor to provide hardware in the event of a disaster or determine if data should be mirrored to hardware placed at a location outside the data center.

Recommendation

22. **ISD management investigate the feasibility of obtaining an agreement with a vendor to provide hardware in the event of a disaster or determine if data should be mirrored to hardware placed at a location outside the data center.**

COMDISCO Study

Driven by concerns about the viability of the ISD's data center, the Board of Supervisors approved the CAO's Asset Management Plan in November of 1998. The Asset Management Plan stated that all County data centers would be studied to determine the feasibility of consolidating them into one data center maintained by ISD. In addition, ISD's current data center was examined to determine if it was suitable for use as the County's primary data center.

COMDISCO was the vendor retained to perform the feasibility study. Their report concluded that ISD's data center is not suitable for use as the County's primary data center, and does not meet the requirements of an "essential facility." An essential facility, as defined by the Uniform Building Code, is one that can resist a lateral force that is 50% greater than that required of a regular office building. It also must be

provisioned to withstand the loss of utility power by employing a dual input power solution, dual generators and dual uninterruptible power supplies. The report indicates the existing data center's support structure would likely fail in the event of an earthquake, causing the facility to "pancake" onto the first floor, collapsing the data center and its contents. According to the feasibility study, it would be more cost effective to build a new data center rather than renovate the current data center to meet standards of an essential facility. The COMDISCO Report includes a total of 54 recommendations that identified deficiencies that warranted immediate attention. ISD reported the following recommendation status: Implemented 15 (28%), In Process 12 (22%), and No Action 27 (50%).

The CAO, ISD and DPW are currently in the process of planning a new data center and estimate it will take three to five years to obtain a completed facility. In the interim, we noted ISD has taken measures to upgrade their current data center facility with those recommendations from the COMDISCO Report that are cost beneficial

Recommendation

None.

Additional Issues

Power Outages

As a result of recent power outages, ISD management identified single points of failure in the power generators, uninterruptible power supply (UPS), and distribution systems. These single points of failure could cause an interruption of critical business processes. Therefore, ISD Management should conduct a cost benefit analysis to determine the feasibility of eliminating the single points of failure in the power generators, UPS, and distribution systems at its existing data center.

Recommendation

- 23. ISD management conduct a cost benefit analysis to determine the feasibility of eliminating the single points of failure in the power generators, UPS, and distribution systems at its existing data center.**

Intrusion and Detection

Computer hacking, virus infections and vandalism are a constant concern for the County. These incidents can result in disclosure, corruption and/or destruction of County data. Even if data are not destroyed, access to it may be denied for hours or days, impacting vital County processes.

In 1999, the Los Angeles Municipal Court website was vandalized. The website was defaced and although there were no serious business disruptions reported, the incident served as an indication of the County's vulnerability to computer hacking. The risk of similar occurrences is rising due to the County's increased dependence on the Internet. There is growing concern about privacy and the protection of County information

transmitted over the Internet or maintained in databases. Consequently, intrusion detection (ID) systems are important to alert management to computer hacking.

An ID system is a type of security management system that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches. According to ITS Data Security, an ID system is currently not utilized in the security infrastructure. ISD primarily relies on software and passwords to protect access to mainframe computing resources. ISD management understands the importance and need for ID systems, but cites competing priorities, cost, lack of knowledge and dedicated resources as reasons that prevent the implementation of an ID system.

Without an ID system, active monitoring and analyzing of both user and system activities cannot be performed and ISD is not able to detect security breaches that might be occurring. Therefore, ISD management should evaluate the feasibility of acquiring an intrusion detection system to integrate with the existing security infrastructure.

Recommendation

- 24. ISD management evaluate the feasibility of acquiring an intrusion detection system to integrate with the existing security infrastructure.**

Attachment A

Components of an Effective Disaster Recovery Plan


**Included in
ISD's DRP**

<p>A.) <u>Key Decision-Making Personnel</u></p> <p>Telephone directory of key decision-making personnel to be notified in the event of a disaster. Does the directory include:</p> <ul style="list-style-type: none"> ➤ Primary and emergency telephone numbers and addresses for each contact person. ➤ Phone numbers & addresses for: <ul style="list-style-type: none"> • Representatives of equipment & software vendors • Contact persons at recovery facilities including hot-site reps • Contact persons at off-site media storage facilities and the contact persons within the company who are authorized to retrieve media from off-site facility 	<p style="text-align: center;">Yes</p> <div style="text-align: center;">↓</div>
<p>B.) <u>Required Supplies</u></p> <p>All supplies required for continuing normal business activities should be maintained, including 1) a detailed up-to-date hardcopy procedure that can be easily followed by contract personnel who are unfamiliar with standard operations. 2) a supply of special forms such as check stock, invoice forms order forms, etc.</p>	<p style="text-align: center;">No</p>
<p>C) <u>Planning & Reconstruction Methodologies</u></p> <p>1. Reconstruction</p> <ul style="list-style-type: none"> A. <u>Organization & Assignment of Responsibilities</u> should exist which include decision-making IS & user personnel. These individuals lead teams that respond to critical functions or tasks defined in the plan. B. <u>Emergency Action (First Response) Team</u> ensures orderly evacuation of personnel and securing human life. C. <u>Damage Assessment Team</u> assesses the extent of the damage following the disaster. 	<p style="text-align: center;">Yes</p> <div style="text-align: center;">↓</div>

Attachment A

Components of an Effective Disaster Recovery Plan

Included in
ISD's DRP

<p>Planning and Reconstruction (continued)</p> <p>D. <u>Emergency Management Team</u> coordinates the activities of all recovery teams & handles key decision-making. This team is the “overseer” and coordinates the following activities:</p> <ul style="list-style-type: none"> ➤ Retrieving critical data from off-site storage ➤ Installing & testing systems software and applications at the hot-site ➤ Identifying, purchasing and installing hardware at the system recovery site ➤ Operating from the system recovery site ➤ Rerouting network communications traffic ➤ Reestablishing the user/system network ➤ Transporting users to the recovery facility ➤ Reconstructing databases ➤ Coordinating systems use and work schedules <p>E. <u>Security Team</u> assesses the systems security and communications links.</p> <p>F. <u>Emergency Operations Team</u> individuals oversee operations at the hot-site.</p> <p>G. <u>Network Recovery Team</u> is responsible for rerouting wide area voice and data communications traffic & reestablishing host network control and access at the recovery site.</p> <p>H. <u>User Hardware Team</u> locates and coordinates the delivery and installation of user terminals, printers, photocopiers & other necessary equipment.</p>	<p style="text-align: center;">Yes</p> <div style="text-align: center;">  </div>
<p>D) Risk Evaluation</p> <p>1. Risk Ranking</p> <p>List of critical applications ranking from highest to lowest priority, required recovery times. The identification of critical systems usually results from a formal exercise in risk analysis coordinated by both information systems processing and end user personnel. Typical rankings are:</p> <p>Critical - These functions cannot be performed unless they are replaced by identical capabilities. Tolerance to interruption is very low, cost of interruption is very high.</p> <p>Vital - These functions can be performed manually, at tolerable costs.</p> <p>Sensitive - These functions can be performed manually, at tolerable costs, for an extended period of time with use of additional</p>	<p style="text-align: center;">No</p>

*AUDITOR-CONTROLLER
COUNTY OF LOS ANGELES*

Attachment A
Components of an Effective Disaster Recovery Plan

**Included in
ISD's DRP**

<p><u>Risk Evaluation (continued)</u></p> <p style="padding-left: 40px;">staff to perform processes.</p> <p>Non-Critical - These functions can be interrupted for an extended period of time, at little or no cost and require no catching up when restored.</p> <p>2. Business Impact Assessment (BIA)</p> <p>A BIA of all business units that are part of the business environment enables the team to: identify critical systems, processes and functions; assess the economic impact of incidents and disasters that result in a denial of access to systems and other services and facilities; and assess the "pain threshold," that is, the length of time business units can survive without access to the systems, services, and facilities.</p> <p>The BIA is a proven method of determining the cost of risk. It can assist in developing a disaster recovery and business continuity planning process in an expeditious and cost-effective manner.</p>	<p style="text-align: center;">No</p> <p style="text-align: center;">↓</p> <p style="text-align: center;">No</p>
<p><u>E) Critical Recovery Time Period</u></p> <p>What is that window of time which business processing must be resumed before suffering significant or unrecoverable losses?</p> <ul style="list-style-type: none"> ➤ Applications to Recover in Critical Time Period ➤ User and Data processing interrelationships ➤ Processing Priorities 	<p style="text-align: center;">No</p>
<p><u>F) Off-Site Facilities</u></p> <ul style="list-style-type: none"> ➤ Security & Control of Off-site facilities – Facility needs to be safely secure ➤ Media & Documentation Backup <ul style="list-style-type: none"> • Periodic Backup Procedures should exist • Frequency Rotation to ensure all data is captured • Operation Procedures like operating system manuals • System & Program Documentation • A copy of the current Disaster Recovery Plan • Record keeping of off-site storage 	<p style="text-align: center;">Yes</p> <p style="text-align: center;">↓</p>
<p><u>G) Alternate Computer Hardware and Software Requirements</u></p> <ul style="list-style-type: none"> ➤ Hot-sites- fully configured and ready to go in a few hours. Contract provisions should include: <ul style="list-style-type: none"> • Hardware Configurations • Speed of Availability 	<p style="text-align: center;">Yes</p>

*AUDITOR-CONTROLLER
COUNTY OF LOS ANGELES*

Attachment A

Components of an Effective Disaster Recovery Plan

**Included in
ISD's DRP**

<p><u>Alternate Hardware and Software Requirements (continued)</u></p> <ul style="list-style-type: none"> • Usage Period • Communications adequate • Testing rights included • Reliability of vendor & sites offered • Duplicate Information Processing Facility – These are dedicated, self-developed recovery sites that can backup critical applications. 	<p style="text-align: center;">Yes No Yes Yes No ↓</p>
<p><u>H) Telecommunications Network</u></p> <p>The Disaster Recovery Plan should include a telecommunications component. There should be adequate capabilities to maintain critical business processes. Telecommunications include telephone voice circuits, wide area networks and local area networks. Telecommunication continuity should include:</p> <ul style="list-style-type: none"> ➤ Redundancy - which involves providing a second cable/connection, through an alternate route, for use in the event the primary event is damaged. ➤ Alternative Routing- is the method of routing info via an alternate medium such as copper cable or fiber optics in different networks, circuits or end points should the normal network be unavailable. Other examples include use of microwave communication. ➤ Count- The number of records that were carried to the backup site versus the number required. Also, ensure the number of critical systems that were successfully recovered can be measured. ➤ Accuracy- Compare accuracy of output results with those for the same period processed under normal conditions. 	<p style="text-align: center;">No</p> <p style="text-align: center;">↓</p>
<p><u>I) Business Continuity Testing</u></p> <p>Although full-scale testing may not be feasible, there should be partial testing to determine how well the plan works or which portions of the plan need improvement.</p> <p>1. Specifications</p> <p>Tests should include:</p> <ul style="list-style-type: none"> ➤ Key recovery team members ➤ Include critical components ➤ Simulate actual prime-time processing conditions ➤ Verify the completeness and precision of the Disaster Recovery Plan information ➤ Evaluate the performance of the personnel involved in the exercise ➤ Evaluate the coordination between the business continuity team and external vendors ➤ Measure the ability and capacity of the backup site to perform 	<p style="text-align: center;">Yes for Unisys No for IBM</p> <p style="text-align: center;">↓</p>

*AUDITOR-CONTROLLER
COUNTY OF LOS ANGELES*

Attachment A

Components of an Effective Disaster Recovery Plan

**Included in
ISD's DRP**

<p><u>Business Continuity Testing (continued)</u></p> <p>prescribed processing</p> <ul style="list-style-type: none"> ➤ Measurement of the overall performance of operational and information systems processing activities related to maintaining the business entity <p>2. Test Execution- The testing should include the following test phases:</p> <ul style="list-style-type: none"> ➤ Pretest- Identify the set of actions necessary to see the stage of the actual test. ➤ Test- this is the actual test of preparedness to respond to an emergency. Operational activities are executed to test the specific objectives of the Disaster Recovery Plan. ➤ Post-Test- Formal evaluation of the plan & implementing indicated improvements. <p>3. Documentation of Results- Every phase of the test should include detailed documentation of observations, problems & resolutions.</p> <p>4. Results Analysis- There should be ways to measure the success of the plan and test against the stated objectives. The results should include:</p> <ul style="list-style-type: none"> ➤ <u>Time</u> elapsed for completion of prescribed tasks ➤ <u>Amount</u> of work performed at the backup facility by clerical staff and information systems processing operations. ➤ <u>Count-</u> The number of records that were carried to the backup site versus the number required. Also, ensure the number of critical systems that were successfully recovered can be measured. 	<p style="text-align: center;">Yes for Unisys No for IBM</p> <div style="text-align: center;">↓</div>
<p><u>J) Disaster Recovery Plan Maintenance</u></p> <p>Plans and strategies should be reviewed and updated on a scheduled basis to reflect continuing recognition of changing requirements. A Disaster Recovery Plan coordinator should maintain the Disaster Recovery Plan. The coordinator's responsibilities should include:</p> <ul style="list-style-type: none"> ➤ Development of a schedule for periodic review and maintenance of the plan advising all personnel of their roles and deadlines for receiving changes ➤ Arrange and coordinate scheduled and unscheduled tests for the Disaster Recovery Plan to evaluate its adequacy ➤ Participate in the scheduled plan tests performed at least once per year on specific dates 	<p style="text-align: center;">No</p> <div style="text-align: center;">↓</div>



COUNTY OF LOS ANGELES

Internal Services Department

9150 East Imperial Highway
Downey, California 90242



United We Stand

JOAN OUDERKIRK
Director

TELEPHONE: (562) 940-2901
FACSIMILE: (562) 803-0724

May 23, 2002

To: J. Tyler McCauley
Auditor-Controller

From: Joan Ouderkirk
Director

Subject: **FINAL DRAFT REPORT ON REVIEW OF DISASTER RECOVERY PLAN**

ISD has reviewed the Final Draft Report on Review of Disaster Recovery Plan provided by your staff. ISD agrees with the direction of the recommendations and will be pursuing their implementation. Because we have made significant efforts in this area already, it is clear that ISD's ability to respond will be limited by funding available.

Most critical to ISD is protection of the data and systems through the physical integrity of the data center that houses them and backup provisions should a disaster occur. ISD has sought funding for this purpose and has advised the CAO and the Board that these are critical needs unmet in the proposed 2002-2003 County budget. For several years we have advocated the need to replace the existing data center with a stronger, more resilient facility. Funding is the key issue for the following items essential to protection of our data and systems:

- Mirroring of Data and Applications

ISD's review of disaster recovery methods indicates that the most reliable and timely backup/recovery method is to duplicate data in real time at a remote site that includes a redundant computer configuration, mirroring. The unfunded need for the establishment of a disaster recovery system that includes mirroring at a geographically remote location for critical County computer systems at the ISD data center is \$3.0 million.

- Resilient Data Center

The first line of defense for data and systems is a facility built to withstand disasters. The existing Downey Data Center does not meet this requirement and it is not cost effective or feasible to upgrade it. A capital project has been initiated and is now in the architectural planning stage to build a new data center. Construction of the new County Data Center to replace the existing Downey Data Center is a critical project that must be completed as planned without delay.

J. Tyler McCauley
May 23, 2002
Page 2

- Improved Data Center Infrastructure

Until a new data center is available, several deficiencies affecting safety and operating stability at the existing Downey Data Center require immediate attention. A consultant study recommended a number of improvements to fire suppression systems, electrical grounding safety, and air conditioning reliability. The unfunded need for these improvements is \$3.6 million.

ISD will be happy to work with the Chief Information Officer to develop Countywide standards for disaster recovery plans and business impact analysis.

I appreciate the dedication and professionalism of your audit staff. Thank you for the opportunity to review and discuss the report. Please call me or have your staff call Mark Gascoigne at 562- 940-2901 should you have any questions.

JO:JK:dg



COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

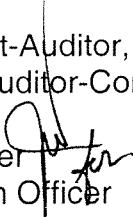
500 WEST TEMPLE STREET
493 HALL OF ADMINISTRATION
LOS ANGELES, CALIFORNIA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

TELEPHONE: (213) 974-2008
FACSIMILE: (213) 633-4733

June 6, 2002

To: Ian Clark
Chief Accountant-Auditor, Audit Division
Department of Auditor-Controller

From: Jon W. Fullinwider 
Chief Information Officer

Subject: **RESPONSE TO AUDITOR-CONTROLLER REVIEW OF INTERNAL SERVICES DISASTER RECOVERY PLAN**

My office has reviewed the Auditor-Controller's (A-C) audit of the Internal Service Department's (ISD) Disaster Recovery Plan. While we are in general agreement with the audit's findings and recommendations, we have identified some issues that need to be addressed.

Business Continuity Planning

The A-C identifies the need to establish countywide Disaster Recovery Planning (DRP) standards for recovering technology assets (systems, networks, applications, and data) in the event of a major disaster. It recommends forming a task force lead by my office charged with developing these DRP standards for Board approval. While countywide DRP standards are important, we believe that this recommendation should be broadened to include Business Continuity Planning (BCP) standards. BCP represents a much broader scope of activities designed to sustain and recover critical work processes during and after a disruption. We believe BCP standards are needed in order to protect County programs and assets. For example, recovering the County's call center technology is futile if the County lacks the personnel to staff the call center itself, or a workplace in which to locate it.

BCP focuses on restoration or sustaining critical business processes and the information technology (I/T) that supports those processes. BCP represents a much broader, cross-functional effort (business process, technology assets and facility) that

spans the entire organization. **At the present time, the County does not have a comprehensive countywide business continuity plan.**

Hot Site Testing

The A-C recommended that ISD pursue with SunGard consolidating their two hot site locations to one locality. We believe that this may be problematic because availability of the services is typically provided on a first-come-first-serve basis. We believe that the A-C should recommend that ISD study the feasibility of consolidating to one location.

Computer Output Services

The A-C made a series of recommendations directed at improving ISD's computer output recovery capabilities, but did not identify the need for ISD to reestablish vendor contracts for computer output availability services. At one time, ISD had contracted for computer output services covering 40 percent of its total workload. Currently, ISD does not have a contract with any vendor that would provide output services in the event a disaster disables the data center. Putting these vendor contracts in place would mitigate the County's exposure in this area.

Telecommunications Recovery and Network Infrastructure

The A-C made several recommendations regarding redundancies and bandwidth requirements for the LANET – the County's wide area network. We believe the network redundancies and bandwidth requirements are being addressed with the implementation of the County's new Enterprise Network (EN). The EN is being implemented in conjunction with the Carrier Services Agreement with Pacific Bell for telephone services.

Intrusion Detection

The A-C recommended ISD evaluate the feasibility of acquiring an intrusion detection system. The County has established a Cyber Terrorism Task Force charged to develop a countywide security architecture. A task force workgroup focused on network strengthening has begun the process of identifying and acquiring intrusion detection software. This process is scheduled for completion by the end of the month.

If you have any questions, please contact Jonathan Williams at (213) 974-2080.

JWF:GM:jsl